David M. Given (State Bar No. 142375)
Nicholas A. Carlin (State Bar No. 112532)
PHILLIPS, ERLEWINE & GIVEN LLP
50 California Street, 32nd Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911
Email: dmg@phillaw.com
nac@phillaw.com

James M. Wagstaffe (State Bar No. 95535)
Michael Ng (State Bar No. 237915)
Michael von Loewenfeldt (State Bar No. 178665)
Ivo Labar (State Bar No. 203492)
KERR & WAGSTAFFE LLP
100 Spear Street, 18th Floor
San Francisco, CA 94105–1528
Telephone: (415) 371-8500
Fax: (415) 371-0500
Email: wagstaffe@kerrwagstaffe.com
mng@kerrwagstaffe.com
mvl@kerrwagstaffe.com
labar@kerrwagstaffe.com

Interim Lead Counsel for Plaintiffs
[ADDITIONAL COUNSEL LISTED BELOW]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE:

APPLE IDEVICE ADDRESS BOOK LITIGATION

Case No. 13-cv-00453-JST

CLASS ACTION

OPPERMAN PLAINTIFFS' OPPOSITION TO APPLICATION DEVELOPER DEFENDANTS' MOTION TO DISMISS CONSOLIDATED AMENDED CLASS ACTION COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

Hernandez v. Path, Inc., No. 12-cv-1515-JST
Pirozzi v. Apple, Inc., No. 12-cv-1529-JST
Gutierrez v. Instagram, Inc., No. 12-cv-6550-JST
Espitia v. Hipster, Inc., No. 4:13-cv-432-JST
(collectively, the "Related Actions")

Date: January 22, 2014
Time: 9:30 A.M.
Courtroom: 9, 19th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Pages

Cases

Statutes

Other Authorities

Rules

a)

I. INTRODUCTION

For quite some time, many of the most popular "apps" used on Apple's now ubiquitous iPhones, iPads, and iPod touches (collectively "iDevices") were secretly transmitting a user's private address book, known as the Contacts, over the Internet. Plaintiffs bring this class action against Apple and several application developers (the "App Defendants") challenging this unlawful theft of Plaintiffs' and other customers' private information on a variety of statutory and common law grounds. Four groups of motions to dismiss were filed. This opposition responds to the Application Developer Defendants' Joint Motion to Dismiss (Dkt. No. 396) as well as Twitter's repetitive joinder (Dkt. No. 397) and the motion to dismiss by Defendants Chillingo, ElectronicArts, Rovio, and Zeptolabs (Dkt. No. 393).

The App Defendants collectively spend 60 pages making basically four arguments. First, they argue that consumers suffer no legally cognizable injury when their Contacts are copied without permission from their iDevices. Second, the App Defendants insist that they had permission to copy the Contacts and did not misuse them in any way. Third, the App Defendants insist that Plaintiffs' Consolidated Amended Complaint ("CAC"), which provides far more detail than the pleading rules require, is somehow too cursory or indefinite for the App Defendants to defend this lawsuit. Finally, the App Defendants insist that the alleged conduct does not fall within any of the legal theories alleged in the case.

The App Defendants' motions fall far outside the proper bounds of Rule 12(b). Replete with adjectives, they read more like a jury argument than a pleading motion. The App Defendants' assertions that no harm occurred, and that they had permission, either ignore the pleaded facts (and their prior public apologies) or ask the Court to disbelieve them, neither of which is proper at this stage without an evidentiary record. Moreover, these defendants present a cramped reading of both applicable law and the CAC's allegations, none of which should be accepted by the Court.

Each contention is discussed below. At bottom, the App Defendants cannot escape liability for stealing Plaintiffs' contacts by calling that conduct a "social media function" and

insisting that so long as data is only copied, not destroyed, and Plaintiffs are not aware (without discovery) of any specific further misuse of the data once copied, no legal violation occurs.

II. RELEVANT FACTS

The basic factual allegation against the App Defendants is quite simple: Each, with the assistance and knowing participation of Apple, designed and distributed an app for iDevices. The apps, which performed various functions, all have one thing in common: Each app caused the iDevice to access the iDevice owner's address book (Contacts) associated with the pre-installed Apple Contacts app and then transmit a copy of each user's Contacts to the App Defendant. All apps named in this suit did this wholly without permission or warning. Some apps had screens or menus prompting a user to (according to App Defendants) "find friends," but they never sought permission to transmit the Contacts to an App Defendant's server, or even explained that such would be done. The transmission of data was made publicly in an unencrypted form, subjecting iDevice users to the public exposure of their private materials to everyone within range of their device's broadcast. This violated the privacy and property rights of iDevice users, depleted their iDevice resources, and otherwise damaged users.

These allegations are described in great detail in the CAC. Plaintiffs are 16 individuals who purchased iDevices from Apple, Inc. prior to February 2012, which they used to maintain their mobile address books. (CAC ¶¶ 10, 16-32, 126, 157-59, 463, 641-48, 658.) One of the "game changing" aspects of the iDevice was Apple's decision to manufacture and market secure "smart devices" that not only function as a phone, music player, or tablet, but also manage one's address book and calendar, receive email, and function as portable computers running an almost unlimited number of software applications which Apple calls "apps." (CAC ¶¶ 83-86.)

In contrast to its competitors, Apple exerts nearly total control over software that can be installed on its devices. (CAC ¶ 184.) Apps for iDevices can be obtained only through Apple's centralized "App Store," and the company exercises strict controls over what apps can be offered there. (CAC ¶¶ 174-75.) In addition to running the App Store and receiving a substantial portion of fees for each app sold, Apple also serves as agent for each App Defendant with respect

to the marketing, sale, deployment and account processing of their respective iDevice apps. (CAC ¶ 145.)

Since the iDevices were introduced, Apple has engaged in an aggressive and sustained advertising effort to convince the public that iDevices are secure, and that private materials maintained on the iDevice cannot be accessed by any other installed apps, much less surreptitiously transmitted without the user's knowledge and consent. (CAC ¶¶ 121-27.) As described in the accompanying opposition to Apple's motion to dismiss, these various advertisements intentionally created the clear—but erroneous—impression that an iDevice is a secure platform for keeping and managing private materials and property. (Id.)

The iDevices come with a built-in "Contacts" feature which permits the user to keep and maintain personal and private information about the user, the user's family, friends and business contacts, or anyone else. (CAC ¶ 159.) Akin to a rolodex or traditional "little black book," the Contacts of each user reveals connections, associations and relationships that are unique to the owner of the iDevice. (CAC ¶ 160.) Apple explicitly reminded and instructed all App Defendants that "the Address Book database is ultimately owned by the [iDevice] user" (CAC ¶¶ 205; Dkt. No. 1-2 at 25) and, not surprisingly, consumers and numerous studies place significant monetary value on their Contacts. (CAC ¶ 645.) The investment of time, effort, skill and creative energy used to build the user's unique address book has independent value. (CAC ¶¶ 160,165.) It is also abundantly clear that private Contacts address books are a highly valued surveillance target because companies (like these Defendants, for example) can use such address books to profit from and exploit emerging social media through advertising and/or expanding their own user data bases. (CAC ¶¶ 168-171.) Similar lists of addresses, telephone numbers and email addresses are commodities that are available for sale in the marketplace. (CAC ¶¶ 151, 645.)

As a result of sustained advertising assurances from Apple, each Plaintiff purchased his/her iDevice with the expectation that he/she would be able to utilize the "Contacts" function and add-on apps available through the App Store without compromising the privacy, safety or exclusive control of Plaintiffs' Contacts or other personal and private information. (CAC ¶ 32.)

Had any Plaintiff known that iDevices lacked promised features or that Apple designed the iDevices with known vulnerabilities to unauthorized operations from Apple-issued (third-party) apps, Plaintiffs would not have accepted add-on apps from Apple or the App Store, and would have paid less for his or her iDevice or not have purchased it. (CAC ¶¶ 32, 64, 125-127.)

During the timeframe at issue, Plaintiffs received a number of apps from the App Store, including apps jointly manufactured by the App Defendants and Apple. (CAC ¶¶ 16-31.) These include some of the most popular "free" apps, like *Twitter*, *Instagram*, and *Yelp!*, as well as popular games like *Angry Birds* and *Cut the Rope* which had both free and paid versions. (CAC ¶¶ 328, 370, 387.) Plaintiffs also maintained substantial private Contacts on their iDevice; each Plaintiff had more than one hundred contacts in their iDevice Contacts at all relevant times. (CAC ¶¶ 10, 16-32, 126, 157-59, 463, 641-48, 658.)

Unbeknownst to Plaintiffs, many popular apps, including the ones at issue here, were not benign social media tools or games. They were active surveillance programs designed to intercept a users' private information without the users' knowledge or consent. (CAC ¶¶ 62, 107-119.) This surveillance took two forms.

First, some apps simply caused iDevices to transmit the materials without even a pretense of permission. For example, in early February 2012, it was revealed that defendant Path's eponymous app was uploading data stored on users' Apple Devices (including Contacts and calendar) to its servers, causing Path's CEO to issue a public apology to Path users. (CAC ¶ 110.)

Second, other apps misled users into triggering the theft of their data through activation of unexplained features that offered to identify "friends" in one's Contacts who used the same app. (CAC ¶¶ 108, 113.) The App Defendants, and especially the Chillingo movants, lean heavily on this mislabeled "friend finder" feature in their motions, never revealing to the Court that the so-called permission was *not* requested to *obtain* the Contacts or to send a copy of those contacts to the App Defendants' servers. (CAC ¶¶ 107-117.) Users who were asked whether they wanted to know if their "friends," for example, also played *Angry Birds* or used *Twitter*

were never told that by triggering that app function the App Defendant would obtain without restrictions all of their private Contacts. (CAC ¶¶ 111, 117.)

Either way, iDevices running these apps transmitted the stolen private materials from the iDevices to their makers' computer servers. (CAC ¶¶ 1, 7, 9, 62-64, 107, 11-13, 115, 118, 123, 130-36, 138, 438, 649-56.) That transmission not only stole and publicly disclosed the user's Contacts, it also used iDevice system resources, including energy and battery life, WiFi bandwith, or cellular time. (CAC ¶ 147.) Battery life is of particular concern to owners of iDevices because the battery on an iDevice cannot be replaced. (CAC ¶¶ 147, 338.) Because any use of a battery drains it, and rechargeable batteries have a finite number of charges they will take, any use of an iDevice necessarily decreases not only the life of the battery but of the device itself. (Id.) Moreover, many of these surreptitious transmissions appear to have been made without industry standard encryption. (CAC ¶¶ 146, 232-233, 319, 341, 363.) Sending these private materials on an unencrypted radio broadcast (by either WiFi or cellular network) and via the Internet subjects the user to the public exposure of those private materials to innumerable others and also presents a significant risk of additional interceptions by one of many other actors in the surveillance economy.[1] (CAC ¶ 146.) Because no user was warned that the transmission would occur, short of discovery, there is no way for any user to determine how much of his or her Contacts was acquired by third parties other than the Defendants as a result of these unauthorized transmissions. (Id.) Thus each plaintiff, and other users of the same apps, was damaged in a number of ways by the App Defendants' surreptitious actions with his/her Contacts and iDevices. (CAC ¶¶ 129-152.)

[1] For example, Google is in significant legal trouble after it was revealed that Google's mapping vehicles were gathering information from the WiFi of unsuspecting homes as they drove by. See Joffe v. Google, Inc., 729 F.3d 1262, 1263 (9th Cir. 2013).

III. ARGUMENT

A. PLAINTIFFS HAVE STANDING TO PURSUE THEIR CLAIMS

1. Legal Standard Under Rule 12(b)(1)

To have standing under Article III, a plaintiff need only show that (1) it has suffered an injury in fact; (2) that the injury is fairly traceable to the defendants' actions; and (3) the injury will likely be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992). The "injury" requirement does not, however, mean that plaintiff has to win their claim at the beginning of the lawsuit:

> "Injury in fact" [simply] reflects the statutory requirement that a person be "adversely affected" or "aggrieved," and it serves to distinguish a person with a direct stake in the outcome of a litigation—even though small—from a person with a mere interest in the problem.

United States v. Students Challenging Regulatory Agency Procedures (SCRAP), 412 U.S. 669, 690 n. 14 (1973). "The purpose of standing doctrine is to ensure that 'plaintiff's claims arise in a 'concrete factual context' appropriate to judicial resolution and that 'the suit has been brought by a proper party.' The 'injury-in-fact' analysis is not intended to be duplicative of the analysis of the substantive merits of the claim." Haskins v. Symantec Corp., 13-CV-01834-JST, 2013 WL 4516179, *3 (N.D. Cal. Aug. 23, 2013) (quoting Arakaki v. Lingle, 477 F.3d 1048, 1059 (9th Cir. 2007) (internal reference omitted)).

As a threshold matter, Defendants wholly misperceive the standard by which this jurisdictional motion should be determined. When, as here, Defendants have chosen to attack jurisdiction on its face ("facial attacks"), the Court must consider the allegations of the complaint as true. Warren v. Fox Family Worldwide, Inc., 328 F.3d 1136, 1139 (9th Cir. 2003); Gould Electronics, Inc. v. United States, 220 F.3d 169, 176 (3rd Cir. 2000).[2]

---

[2] That Defendants attach declarations does not alter the rule here that this is a facial attack. The declarations do not go to the standing issue and as to Rule 12(b)(6) motions, of course, such materials cannot be considered since they are outside the complaint. Schwarzer, et al., Cal. Prac. Guides: Fed. Civ. Pro. Before Trial ¶ 9:211 (TRG 2013).

Even more fundamentally, where Defendants, as in the present case, dispute the facts underpinning subject matter jurisdiction, and these facts are "inextricably intertwined" with the merits of plaintiffs' claim, in such cases defendants must proceed under Federal Rules of Civil Procedure 12(b)(6) or 56 and "the court should resolve the relevant factual disputes only after appropriate discovery." Kerns v. United States, 585 F.3d 187, 193 (4th Cir. 2009); Augustine v. United States, 704 F.2d 1074, 1079 (9th Cir. 1983). The court may not weigh and decide disputed facts on a facial attack as to jurisdiction. Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004).

The jurisdictional facts and merits are intertwined when "the question of jurisdiction is dependent on the resolution of factual issues going to the merits." Safe Air for Everyone, 373 F.3d at 1040. Courts have referred to this as a "relaxed standard" demanding less jurisdictional proof. S.R.P. ex rel. Abunabba v. United States, 676 F.3d 329, 344 (3rd Cir. 2012).

In the present case, the Article III standing requirements examine the degree to which Plaintiffs have suffered injuries in fact. Plainly, the jurisdictional inquiry here is intertwined with the existence of and degree to which there are compensable injuries. Because Paintiffs' allegations must be accepted as true, and because such factual inquiries await further discovery at a subsequent speaking motion based on evidence, the motion to dismiss here on standing grounds must be denied.[3]

2. Plaintiffs' CAC Establishes Article III Standing

Plaintiffs are suing for Defendants' interception and theft of Plaintiffs' own Contacts address books from Plaintiffs' own iDevices. This is by no means a generalized claim pursued by a party only nominally or spiritually interested in the result. Cf. Drake v. Obama, 664 F.3d 774, 779 (9th Cir. 2011) cert. denied, 132 S. Ct. 2748, 183 L. Ed. 2d 616 (U.S. 2012) (various citizens lacked standing to challenge President Obama's eligibility to be President of the United

[3] Under any circumstances, of course, Plaintiffs must be given leave to amend if the Court is considering granting this motion. See Peterson v. Boeing Co, 715 F.3d 276, 282 (9th Cir. 2013) (leave to amend should be granted with great liberality); Fed. R. Civ. Pro. 15(a).

States); Caldwell v. Caldwell, 545 F.3d 1126, 1133 (9th Cir. 2008) (general interest in informed participation as a citizen did not create standing to challenge teaching of evolution at University of California).

Defendants do not claim that Plaintiffs lack a personal stake in this dispute.[4] Instead, Defendants make "standing" arguments based on their assertions that they did not harm Plaintiffs when they copied their Contacts. That is a disguised merits attack. Before responding to Defendants' specific arguments, Plaintiffs will first identify the claims and remedies Defendants ignore in their motion.

First, the App Defendants ignore Plaintiffs' requests for prospective injunctive relief to stop the challenged misconduct. "To have standing to assert a claim for prospective injunctive relief, a plaintiff must demonstrate 'that he is realistically threatened by a repetition of [the violation].'" Melendres v. Arpaio, 695 F.3d 990, 997 (9th Cir. 2012). Because the challenged activity of the App Defendants is a deliberate feature of their apps, it will necessarily continue unless enjoined. Nicacio v. U.S. I.N.S., 797 F.2d 700 (9th Cir. 1985) (noting that on claims for prospective injunctive or equitable relief, "[t]he possibility of recurring injury ceases to be speculative when actual repeated incidents are documented" and establishes standing to redress that prospective harm) (overruled on separate grounds in Hodgers-Durgin v. de la Vina, 199 F.3d 1037, 1045 (9th Cir. 1999)).

Second, the App Defendants ignore Plaintiffs' claims for statutory damages. (CAC ¶ 609.) "[T]he injury required by Article III can exist *solely* by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" Edwards v. First American Corp., 610 F. 3d

---

[4] In a putative class action like this one, standing need only be established for one class representative (of which there are sixteen prospects here). As this Court recently reaffirmed, "[the Ninth Circuit's] [standing] law keys on the representative party, not all of the class members, and has done so for many years.'" Lilly v. Jamba Juice Co., 13-CV-02998-JST, 2013 WL 6070503, *2 (N.D. Cal. Nov. 18, 2013) (citing Stearns v. Ticketmaster Corp., 655 F.3d 1013, 1021 (9th Cir. 2011) cert. denied, 132 S.Ct. 1970 (U.S. 2012); see also Bates v. United Parcel Serv., Inc., 511 F.3d 974, 985 (9th Cir. 2007) (en banc) ("[i]n a class action, standing is satisfied if at least one named plaintiff meets the requirements")).

514, 517 (9th Cir. 2010) (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)), writ dism'd, 132 S. Ct. 2536 (June 28, 2012)) (per curium). Thus, if any statute prohibits any of the Defendants' conduct and allows for a civil recovery, Plaintiffs have demonstrated an injury sufficient to satisfy Article III. Id. Here, Plaintiffs allege the violation of numerous statutes as discussed throughout the CAC.

Instead of addressing these claims, or really any of the claims specifically, the App Defendants quibble over what remedies may be available and assert that there is no "injury in fact." Perhaps the most specious argument is the App Developers' claim that private Contacts lists have no value, and the theft of them does not create a particularized injury. Not only is that a disguised merits argument, it is nonsense. Any alleged trespass upon property or invasion of privacy triggers constitutional standing. See F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 281 (2008) (explaining that damage is presumed in trespass actions). Thus, Defendants' intrusion into each Plaintiff's private iDevice address book and their disclosure (to themselves and/or others via the internet) of each Plaintiff's private data constitutes injury in and of itself for standing. As alleged, without Plaintiffs' consent, these Defendants *took* something that wasn't theirs (Plaintiffs' iDevice address books), *used* something that wasn't theirs (Plaintiffs' iDevices, iDevice resources and private iDevice address books), or helped their co-defendants do so, despite public assurances to the contrary. (CAC ¶¶ 7, 8, 24, 31, 62, 63, 107-120, 130-134, 232, 238, 245, 259, 261, 301, 315, 352, 358, 363, 376.) The associated injuries to Plaintiffs and their properties are not future, nor remote, nor "speculative;" instead, they have already occurred and Plaintiffs and their property *were* impacted.[5]

[5] The App Defendants are very careful *not* to state that they did not keep or misuse the data they took; they only say that there are no such allegations in the Complaint. App Defendants are plainly wrong; such allegations permeate the CAC. (CAC ¶¶ 110, 259, 266, 268, 296, 306, 320-21, 351, 358, 363, 374-76, 393-96; see also Dkt. No. 194-8.) Plaintiffs are frankly not yet in a position to establish other than from Defendants' public admissions whether there were more grevious violations of their rights (such as warehousing their data, or selling, or transferring, or re-directing it). (CAC ¶¶ 374-75, 392-94.) That is the nature of surreptitious data theft. While the taking of the materials alone creates standing, Plaintiffs are entitled to discovery to determine the full scope of what was done with their materials. It will be no surprise to anyone if it turns

The district court cases cited by the App Defendants are inapposite. They concern automatically-generated computer data sets (e.g., internet search history (LaCourt v. Specific Media, Inc., SACV 10-1256-GW(JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011)); web pages visited that have no physical world equivalent (In re iPhone Apple Lit., 844 F. Supp. 2d 1040 (N.D. Cal. 2012)); iterant data points (e.g., a device's unique identifier (Low v. LinkedIn, No. 11-CV-01468-LHK, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011)); or the owner's own phone number, email, address or other identifying information (In re Jet Blue, 379 F. Supp. 2d 299 (E.D.N.Y. 2005))). A personal address book created by a Plaintiff is clearly property belonging to the Plaintiff and in which she has a right of privacy. U.S. v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ("[C]ell phones contain . . . private information, including . . . address books, and . . . owner[s] ha[ve] a reasonable expectation of privacy regarding this information."); — contacts were purposefully and personally made (CAC ¶ 681), have a physical world equivalent — the theft of which would plainly be actionable — and are a collection of information that forms a unique database specific to each plaintiff. Apple itself recognizes that Contacts belong to the user, and their economic value is clear. (CAC ¶¶ 151, 160-71, 205, 645.)

The App Defendants' other arguments are equally without merit. Plaintiffs have alleged that Defendants' conduct caused a use of battery life, energy, cellular time, storage space, and bandwidth. (CAC ¶ 147.) None of those are costless or infinite resources.[6] The App Defendants' assertion that Plaintiffs are required to allege specifically which computer code caused what amount of resource use is baseless. Unlike the generic allegations in the cases movants cite, here Plaintiffs have alleged specific conduct—intercepting and broadcasting the

---

out that one or more of the App Defendants engaged in further misconduct once they obtained Plaintiffs' materials.

[6] It is movants' assertion that each Plaintiff must allege specifically how much sooner she had to charge her phone or replace her iDevice that is implausible. Do movants seriously expect the Court to believe that their apps sent data to movants' servers wirelessly *without* using electricity, system resources, or battery life? This is precisely the type of argument that makes a mockery out of both standing law and the basic function of a pleading: to let the Defendants know enough about the suit so that they can defend it.

Contacts—that caused loss of system resources. No controlling authority requires that the amount of loss be large to create standing. Indeed, the opposite is true. Cramer v. Skinner, 931 F.2d 1020, 1027 (5th Cir. 1991) ("The Constitution draws no distinction between injuries that are large, and those that are comparatively small." [An] "'identifiable trifle' is sufficient injury to establish standing; standing is not 'to be denied simply because many people suffer the same injury.'" (quoting SCRAP, 412 U.S. at 686-87, 689 n. 14)).

Finally, Plaintiffs have alleged that they will incur costs removing the malware at issue from their computers. The same allegation was already found to create standing against Path. Hernandez v. Path Inc., 12-CV-01515, 2012 WL 5194120, *2 (N.D. Cal. Mar. 26, 2013). The assertion that Plaintiffs are wrong is not a valid argument either on standing or on a motion to dismiss.

Plaintiffs are not interlopers, bystanders, or gadflies. They are bringing suit for numerous violations of their own rights by these specific defendants. They clearly have a sufficient interest in this suit to trigger Article III standing.

B. PLAINTIFFS' CAC ADEQUATELY ALLEGE FACTS TO SUPPORT ALL CLAIMS

1. Legal Standard Under Rule 12(b)(6)

A party's complaint need *merely be plausible* on its face, offer more than labels and conclusions, and provide some factual basis in support of its claim. "[D]etermining whether a complaint states a plausible claim is context-specific, requiring the reviewing court to draw on its experience and common sense." Ashcroft v. Iqbal, 556 U.S. 662, 663-64 (2009). Because Plaintiffs are unlikely before discovery to have access to Defendants' internal documents or other secret company knowledge without discovery, only "minimal factual allegations should be required at the motion to dismiss stage." Thomas v. City of Galveston, Texas, 800 F. Supp. 2d 826, 844 (S.D. Tex. 2011); EQT Infrastructure Ltd. v. Smith, 861 F. Supp. 2d 220, 231 (S.D.N.Y. 2012) (Rule 8 "should not be turned into 'an insurmountable hurdle,' particularly where some of the relevant facts are within the exclusive knowledge or control of the defendants").

2. California Law Applies to Non-California Defendants

Like Apple, Defendants Rovio and Zeptolab argue that people who live outside of California have no standing to sue nonresidents under various California laws,[7] (Dkt. Nos. 393 & 395 at p. 21) even where (as here) the activity that harmed them substantially emanated from California as a result of conduct by them and their California agent. This argument has no merit whatsoever and has been squarely rejected numerous times. See Wang v. OCZ Tech. Group, Inc., 76 F.R.D. 618 (N.D. Cal. 2011); In re Mattel, 588 F. Supp. 2d 1111 (C.D. Cal. 2008). As Judge Wilken explained when Apple made the same argument just a few months ago, this argument:

> "conflat[ed] two issues: the extraterritorial application of California consumer protection laws (or the ability of a nonresident plaintiff to assert a claim under California law), and choice-of-law analysis (or a determination that, based on policy reasons, non-forum law should apply)." Forcellati v. Hyland's, Inc., 2012 U.S. Dist. LEXIS 91393 at *9 (C.D. Cal.). California courts have concluded that "state statutory remedies may be invoked by out-of-state parties when they are harmed by wrongful conduct occurring in California." Norwest Mortg., Inc. v. Superior Ct., 72 Cal.App.4th 214, 224-225 (1999).

In re iPhone 4S Consumer Lit., C 12-1127 CW, 2013 WL 3829653, *7 (N.D. Cal. July 23, 2013); see also Clancy v. Bromley Tea Co., 12-cv-03003-JST, 2013 WL 4081632, *7 (N.D. Cal. Aug. 9, 2013) ("at this early stage of the litigation, 'it would be premature to speculate about whether the difference in various states' consumer protection laws are material in this case.'").

As in that case, here the *Angry Birds/Crystal* and *Cut the Rope/Crystal* Plaintiffs "have [also] alleged that their injuries were caused by [these Defendants'] wrongful conduct ... that originated in California." In re iPhone 4S Consumer Lit., 2013 WL 3829653 at *7. Rovio, ZeptoLab, Chillingo and Apple jointly developed and validated these apps in substantial part in California; they jointly marketed and delivered the apps to consumers from California via the California-based App Store. (CAC ¶¶ 9-10, 14-15, 34-35, 44, 47, 177-78, 182-88, 195-96, 366-412, 428-440.) Thus, Rovio and ZeptoLab are properly subject to Plaintiffs' California statutory

[7] The Motion mentions only California's Unfair Competition Law (UCL) and California Penal Code section 502. (Id.)

claims related to the *Angry Birds/Crystal* and *Cut the Rope/Crystal* apps, as the harmful conduct occurred at least in substantial part in California.

The California Supreme Court's decision in Sullivan v. Oracle Corp., 51 Cal.4th 1191, 1209 (2011), does not mandate dismissal of non-California residents' consumer protection claims for lack of standing. Sullivan is a narrowly decided case involving a certified question from the Ninth Circuit concerning a wage dispute and is therefore not applicable here. See id. at 1207; id. at 1209 (holding that UCL "does not apply . . .*in the circumstances of this case*") (emphasis added). Indeed, given the limitation of the certified question procedure, the Court's decision was narrow and it further distinguished two consumer class actions, because both cases (as here) involved fraudulent misrepresentations originating from California to induce a consumer transaction. See id. at 1208 n.10 (citing Wershba v. Apple Computer, Inc., 91 Cal. App. 4th 224 (2001) and Clothesrigger, Inc. v. GTE Corp., 191 Cal. App. 3d 605 (1987)).

The applicable rule was stated in Wershba, where the California Court of Appeals held that nationwide reach of California consumer law was appropriate where, as here, the defendant was headquartered in California, class members were deceived by representations that were disseminated from California, substantial number of class members were located in California, and decision-making occurred in California. Wershba, 91 Cal. App. 4th at 242.

Any reliance on the Ninth Circuit decision in Mazza v. American Honda Motor Co., Inc., 666 F.3d 581 (9th Cir. 2012) is equally misplaced. Indeed, the court in Bruno v. Eckhart Corp., 280 F.R.D. 540, 546 (C.D. Cal. Mar. 6, 2012) also rejected a similar argument and held that Mazza did not overrule the California Supreme Court's decisions regarding the choice-of-law analysis required under California law, nor could it, because choice-of-law analysis is substantive state law and a state's highest court is the final arbiter on state law. Id. (citing Klaxon Co. v. Stentor Elec. Mfg. Co., 313 U.S. 487, 496 (1941); Fid. Union Trust Co. v. Field, 311 U.S. 169, 177-78 (1940)). "Mazza did not vacate the district court's class certification as a matter of law, but rather because defendant Honda met its burden to demonstrate material differences in state law and show that other states' interests outweighed California's." In re POM Wonderful LLC Mktg. and Sales Practices Litig., ML 10-02199 DDP, 2012 WL 4490860,

*3 (C.D. Cal. Sept. 28, 2012) (finding that plaintiffs met their burden to show that California had sufficient contacts to the claims to ensure application of California law at class certification stage). Thus, the California law claims in this action can be raised against non-residents by plaintiffs living outside of California.

3. Plaintiffs' Unfair Competition Law, Cal. B&P §§ 17200 et seq., Claim Is Properly Pled

The App Defendants argue that Plaintiffs have no standing under the UCL because they did not lose money or property. This argument can only be made by claiming that a person has no property interest in his or her Contacts. None of the "personal information" cases cited by the App Defendants state any such rule. A Contacts address book created and compiled by a Plaintiff is not analogous in any way to "data packets" automatically generated by a computer, other involuntary footprints of Internet use, or someone's name, own phone number or signature.

The App Defendants also insist that there is only a loss of property if the Plaintiff no longer has access to the same data. Such a rule would basically immunize all data theft unless the thief deleted the data after copying it. The App Defendants cite Claridge v. RockYou, Inc., 785 F. Supp. 2d 855 (N.D. Cal. 2011) for this proposition. Claridge involved a data security breach concerning information about the users themselves, not address books owned by the users. The "passed beyond his control or ability to retrieve it" language cited by defendants was a quote from a California appellate case, Silvaco Data Systems v. Intel Corp., 184 Cal. App. 4th 210, 244 (2010), which held that restitution must be available to trigger UCL standing. Silvaco, however, was overruled by the California Supreme Court in Kwikset Corp. v. Superior Court, 51 Cal. 4th 310, 337 (2011); see also Clayworth v. Pfizer, Inc., 49 Cal. 4th 758, 789 (2010). Claridge thus relies on a rejected view of California law and should not be followed by this Court.[8]

[8] Moreover, Plaintiffs have in fact lost the ability to control or retrieve their Contact data taken by the App Defendants.

A basic aspect of a property interest is the right to exclude others from using your property. "One of the main rights attaching to property is the right to exclude others, see W. Blackstone, Commentaries, Book 2, ch. 1, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude." Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000) ("Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property"). That property right was lost here. Indeed, if someone broke into a person's house and photocopied her address book, no one could credibly argue that no dominion or control over property was lost because the book itself was not taken. The fact that the Contacts data was taken electronically – a fact that Defendants universally concede – does not change that result. The App Defendants took these Contacts for a reason. It was not altruistic. And it was not because the Contacts are valueless.

Plaintiffs have also alleged unauthorized use and control over their iDevices (additional property that Plaintiffs own) and a loss of system resources, which have monetary value. They have also alleged that complete and secure removal of the malware in question and validation of the integrity of their iDevices and iDevice data will cost money. The App Defendants' snide assertions that Plaintiffs are wrong do not constitute a ground to dismiss this claim on a 12(b)(6) motion.

Beyond standing, the App Defendants make the cursory assertion that no meritorious UCL claim is pleaded. This is also plainly wrong. First, unless every single statutory claim is dismissed and the recently entered twenty-year *Consent Decree and Order for Civil Penalties* against Path for these same activities is expunged, United States v. Path, Inc., 13-cv-00488 (N.D. Cal. Feb. 8, 2013) (describing Path's violations of the FTC Act through "the automatic collection of information from consumers' mobile device address book"), the UCL claim will survive on its "unlawful" theory. The App Defendants' blithe allegation that they will win every other claim is meritless. Second, Plaintiffs have plainly made sufficient allegations of unfair conduct. The

App Defendants insist *ipse dixit* that taking Plaintiffs' data caused "no plausible harm" and that the "benefit" of a "no-cost service" outweighs any harm. Those are merits questions to be resolved after full discovery concerning the benefits and harms. There is no basis for the suggestion that they can be summarily determined at this stage of the case.[9] The App Defendants' cited cases are inapposite. Davis v. Ford Motor Credit Co., 179 Cal. App. 4th 581 (2009), held that late fees were not unfair where plaintiff could have paid his bills on time. Id. at 598. Smith v. State Farm Mut. Auto. Ins. Co., 93 Cal. App. 4th 700 (2001), held that conduct mandated or authorized by the insurance code could not be "unfair" under the UCL. Id. at 721. Neither supports the App Defendants' request for this Court to summarily deem their alleged conduct "fair" on this motion.

As for the App Defendants' assertion that unfairness must be tethered to a specific law or regulation, that is only one of the applicable tests. See Hutchins v. Bank of Am., N.A., 13-CV-03242-JCS, 2013 WL 5800606, *12 (N.D. Cal. Oct. 28, 2013). "A second line of cases applies a test to determine whether the alleged business practice 'is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers and requires the court to weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim.'" Id. (citations omitted). As discussed above, that determination cannot be made in the abstract on a motion to dismiss in this context.

Plaintiffs have thus properly pleaded their UCL claim against the App Defendants. The motion to dismiss this claim should be denied.

4. Plaintiffs' Computer Fraud Claims Are Properly Pleaded

a) California Computer Crime Law, Cal. Penal Code § 502

Plaintiffs have also properly pled their claims against the App Defendants under

[9] The notion that the App Developers provided a "no-cost service" is simply repetition of the "Big Lie" underlying the electronic surveillance economy. This "service" was plainly a ruse to get Plaintiffs' contacts, not a service at all. Why movants wanted Plaintiffs' contacts will be developed in discovery.

California Penal Code sections 502(c)(1), (2), (6), (7) & (8). Each of the App Defendants' arguments about this claim misreads applicable law.

(1) The App Defendants acted "without permission"

The App Defendants assert that Plaintiffs fail to allege that they acted "without permission" when they (often *automatically and without warning* to Plaintiffs) copied and/or transmitted the contents of Plaintiffs' mobile address books. In so doing, these defendants argue for an unduly narrow interpretation of section 502. Applying the plain language of the statute, it is clear that Plaintiffs have adequately alleged that the App Defendants acted without permission.

The statutory term "permission" should be given its ordinary meaning, i.e., "authorization" or "consent." Plaintiffs have clearly alleged that they have not given authorization or consent to the App Defendants to copy their Contacts. The App Defendants articulate no rationale for their proposed rule that, by downloading an app, an iDevice user gives an app developer permission to access and take for its own the materials or data on a user's iDevice. Their purported authority consists primarily of dicta in a case in which plaintiffs were at least warned in advance of the harm complained of.[10] See In re Apple & ATTM Antitrust Litig., 596 F. Supp. 2d 1288, 1307 (2008) (describing advance warning to users before download). The argument that voluntarily downloading an app implicitly gives permission to conduct other undisclosed access, transfers, and uses of an iDevice owner's Contacts or data has already been found by this Court to be a factual matter and, therefore, not a proper basis for a motion to dismiss. Hernandez, 2012 WL 5194120, at *4.

The correct interpretation of section 502 is that authorization to access a portion of a computer does not imply authorization to access other portions. See, e.g., United States v. Nosal, 08-0237, 2010 WL 934257, *6 (N.D. Cal. Jan. 6, 2010); Weingand v. Harland Financial

[10] The other authority Defendants rely on, In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1068 (N.D. Cal. 2012), which itself relies on ATTM Antitrust, observes only that plaintiffs will have difficulty pleading a legal violation by an app developer whose app was voluntarily downloaded; it does not bar such pleadings as a matter of law.

Solutions, Inc., C-11-3109-EMC, 2012 WL 2327660, *4 (N.D. Cal. June 19, 2012). These cases are more analogous to the facts at bar, which deal with misuse of access to part of a computer, rather than hacking. And that is precisely what has happened here: Plaintiffs gave Defendants at most permission to access their hardware, to install apps promoted as harmless and protective of user privacy, but did not give Defendants unfettered permission to access other private materials, much less off-load their Contacts.

The contention raised expressly in the Chillingo, Electronic Arts, Rovio, and Zeptolab motion to dismiss (Dkt. No. 393), and inferentially in the main motion to dismiss, that permission was granted to some of the App Defendants because some users may have clicked on a "Find Friends" button on certain apps similarly misses the mark. First, clicking a "Find Friends" button is meaningless under the facts pled here, which allege that the Apps had already accessed and transmitted the Contacts information before presenting Plaintiffs with an opportunity to grant or withhold permission. Second, even if the uploading happened after "Find Friends" was selected, the apps did not explain that clicking the "Find Friends" button will result in the copying of the user's Contacts to the App Defendants' servers, or that the transmission will be unencrypted. (CAC ¶¶ 238, 244, 261, 262, 301, 305); Theofel v. Farley-Jones, 359 F.3d 1066, 1073 (9th Cir. 2004) ("an overt manifestation of assent or willingness would not be effective ... if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended." (citing *Prosser & Keeton* § 18, at 119; *cf. Restatement (Second) of Torts* §§ 173, 892B(2))). Even under Defendants' theory, the inquiry is deeply factual, necessitating examination of the disclosures and subsequent conduct. These questions cannot be resolved at the pleading stage.

The App Defendants also argue that "'without permission' means to 'circumvent technical barriers' in order to access or use the information."[11] (App. Defs. MTD at 19.) That

[11] Under this definition, removing items from someone else's home is not theft if the home is unlocked.

overly narrow definition is imported from cases arising in a wholly different context, principally the access of websites and open networks. Multiple decisions by this Court and others have held that circumventing technical barriers is *not* the only way in which a defendant can unlawfully access information "without permission." For example, in Weingand, the court observed that California state case law interpreting section 502 did not limit its applicability to "hackers" who bypassed technical security measures. Weingand, 2012 WL 2327660 at *4 (citing People v. Gentry, 234 Cal. App. 3d 131 (1991)). To the contrary, California precedent established that "authorized access to a portion of a computer system (i.e., its hardware) did not preclude a finding that on [SIC] had obtained unauthorized access to another portion of that system (i.e., its software)." Id. (citing People v. Lawton, 48 Cal. App. 4th 11, 14 (1996)). The Weingand court cited Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007), in which the court did not require plaintiffs to allege circumvention of a technical barrier. Id. at *5.

The purported additional "circumventing technical barriers" element—which appears nowhere in the statute – is drawn from Facebook, Inc. v. Power Ventures, Inc., 08-cv-05780-JW, 2010 WL 3291750 (N.D. Cal. July 20, 2010) ("Power Ventures"). In Power Ventures, the defendant accessed Facebook's website at the behest and with the permission of registered users of both Facebook and Power Ventures' website. In violation of Facebook's terms of use, Power Ventures obtained information about those users as well as other Facebook users. Id. at *7; see also Facebook, Inc. v. Power Ventures, Inc., 08-cv-05780-JF, 2009 WL 1299698, *2 (N.D. Cal. May 11, 2009). The court thus defined the issue before it as "whether an access or use that involves a *violation of the terms of use* is 'without permission' within the meaning of the statute." Power Ventures, 2010 WL 3291750 at *7 (emphasis added); see also id. at *12. That is a very different question than the one before this Court.

The concern in Power Ventures was that a mere violation of a website's terms of use can not constitute criminal unauthorized use of the website because "millions of average internet users access websites every day without ever reading, much less understanding, those websites' terms of use." Id. at *7. The court was concerned that any other rule would essentially permit the people who run websites to invent their own criminal law by creating terms of use that

ordinary people would neither be aware of nor understand. Id. at *9-*11. The court solved this problem in the context of open websites and networks by making a distinction between "access that violates a term of use" and "access that circumvents technical or code-based barriers that a computer network or website administrator erects to restrict the user's privileges within the system, or to bar the user from the system altogether." Id. at *11. The court logically reasoned that a hacker always knows that access is unauthorized. Id. That rule makes sense in the Power Ventures context, but not as a general limitation on section 502. In fact, in cases that do not involve a violation of terms of use, the courts have declined to require this showing. For example, the Weingand court considered and rejected the Power Ventures rationale, noting that the Power Ventures court "did not base its construction of § 502 on any California state court authority or on the statutory language." Weingand, 2012 WL 2327660, at *5. As such, Weingand demonstrates that circumvention of technical barriers is not always required to state a claim under section 502, particularly where the dispute involves the access of individual's computers and computerized devices. See also Synopsys, Inc. v. ATopTech, Inc., 13-CV-02965 SC, 2013 WL 5770542, *11-*12 (N.D. Cal. Oct. 24, 2013); Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087, 1090-91 (N.D. Cal. 2007). This Court should similarly decline to import a "circumvent technical barriers" requirement into section 502.[12] Doing otherwise would render the statute toothless and immunize all forms of invasive malware from liability.

[12] Although the technical barriers requirement is inappropriate in this case, Plaintiffs have nonetheless adequately alleged that the App Defendants have circumvented such barriers. As Plaintiffs have alleged, Apple has represented that third-party apps cannot access iDevice users' private information without the users' express permission (CAC ¶ 64) and that apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used" (CAC ¶¶ 101, 104, 106). Likewise, according to Apple, "[a]ll apps run in a safe environment, so a website or app can't access data from other apps." (CAC ¶ 102.) Using technical barriers to keep apps separate (i.e., to prevent one app from accessing data from another app) is referred to as "sandboxing." (See CAC ¶¶ 3, 209; FAC, Dkt. No. 3, filed May 18, 2012, ¶ 130 and n. 74 (discussing "sandboxed approach to apps" and other methods of securing user data).) Mechanisms to prevent one app from accessing data contained in another are certainly technical barriers as that term was used in Power Ventures. (CAC ¶¶ 122-23.) If such mechanisms exist, yet Defendants' Apps were able, as alleged, to access Plaintiffs' mobile address books before even seeking Plaintiffs' consent to

(2) Plaintiffs have alleged a "computer contaminant

The App Defendants' argument that Plaintiffs have failed to allege a "computer contaminant" also just ignores the plain language of the statute. Section 502(c)(10) defines a computer contaminant as:

> ***any*** set of computer instructions that are designed to modify, damage, destroy, record, or ***transmit information*** within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, ***but are not limited to***, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consumer computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

Cal. Pen. Code § 502(c)(10) (emphasis added). Defendants attempt to narrow this definition to include only "viruses or worms" that "usurp the normal operation of a device." (App Def. MTD at p. 21.) But the statute does not say that; it says "any set of computer instructions," a definition that plainly includes an app. Plaintiffs' have alleged that the App Defendants' apps contain code meeting the statutory definition of a computer contaminant.[13]

b) Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030 (a)(2)(C), (a)(5), & (g)

Defendants also argue that Plaintiffs have not pled that (1) the App Defendants' access of Plaintiffs' iDevices was without authorization or that it exceeded authorized access, or (2) that Plaintiffs suffered loss as that term is defined by the statute. Both arguments are incorrect, and

---

do so (see below), then the only conclusion to be drawn from Plaintiffs' allegations is that Defendants, through their Apps, circumvented technical barriers to access the address books.

[13] The App Defendants' "rule of lenity" argument merely re-states their incorrect statutory interpretation. The rule of lenity does not require courts to ignore the plain language of a statute in favor of complicated, self-interested definitions invented by Defendants. "[T]he rule of lenity is reserved 'for those situations in which a reasonable doubt persists about a statute's intended scope even after resort to the language and structure, legislative history, and motivating policies of the statute.'" United States v. LeCoe, 936 F.2d 398, 402 (9th Cir. 1991) (citation omitted).

the App Defendants' motion should be denied. As discussed above, Plaintiffs' have adequately alleged that the App Defendants accessed Plaintiffs' devices without authorization and in excess of their authorization. See Facebook, Inc., 844 F. Supp. 2d at 1039 n. 43 (citing Multiven, Inc. v. Cisco Sys., Inc., 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) for the proposition that elements of a CFAA claim do not differ materially from the elements of a claim under Section 502). As set forth above, the App Defendants were not authorized to acquire, upload or transmit any portion of Plaintiffs' Contacts.

Plaintiffs have also alleged that they sustained loss in greater than $5,000 as required by the CFAA. Defendants rely on AtPac, Inc. v. Aptitude Solutions, Inc., 730 F. Supp. 2d 1174, 1185 (E.D. Cal. 2010), but in that case the plaintiffs alleged only that the defendant had obtained "something of value in excess of $5,000" without specifying the basis for that alleged loss. In contrast here, Plaintiffs specifically allege that they have sustained losses, such as the value of and de-privatization of the Contacts, the loss in iDevice utility as well as that they will incur significant expenses in connection with removing the computer contaminants from, and validating the integrity of their iDevices. (CAC ¶¶ 146-153, 341, 484, 585, 645.) These allegations are sufficient to plead the requisite loss to state a claim under CFAA.

5. Plaintiff's Wiretap Claims Are Properly Pled

a) ECPA, 18 USC § 2510 et seq.

The Federal Wiretap Act, also known as the Electronic Communications Privacy Act ("ECPA"), makes it a crime and civil violation for any person to, among other things, "intentionally intercept[], endeavors to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). It is similarly a violation of the ECPA to use the contents of an intercepted communication or disclose the contents to any other person. 18 U.S.C. § 2511(1)(c) and (d).

Plaintiffs allege that each of the App Defendants violated the ECPA by surreptitiously causing Plaintiffs' address books from their iDevices to be sent to that Defendant for its use. (CAC ¶¶ 589-609.) The App Defendants move to dismiss, claiming that (a) their theft of the

address book was not contemporaneous with any transmission of it, and therefore not an interception, and (b) that Defendants were the intended recipients of any transmissions they initiated. These arguments ignore the allegations in the complaint and misunderstand applicable law.

Although Plaintiffs have had no opportunity for discovery into the precise mechanism of each defendants' secretive misconduct,[14] Plaintiffs have clearly alleged an interception of an electronic communication. Specifically, Plaintiffs allege that each Defendants' app includes hidden code which autonomously sets into motion the following chain of events: First, the app causes the iDevice to send information from the user's Contacts from the iDevice's storage memory to processors and active memory being used by the app (referred to as an I/O operation). Second, the app then simultaneously intercepts that transmission of the address book and triggers the iDevice to divert, relay and broadcast it across the Internet to that Defendant's servers, where Defendant obtains and possess the Contacts and unilaterally uses it for undisclosed purposes. (CAC ¶¶ 597-599.)

This is clearly a prohibited interception. The ECPA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). An "electronic communication" is broadly defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

Plaintiffs allege that the App Defendants acquired the Contents through the use of hidden code in their apps (clearly an "electronic … or other device") or the apps themselves. The transmission of the Contents between distinct components within the iDevice is a "transfer of …

---

[14] Precisely how, technologically speaking, Defendants got Plaintiffs' private iDevice address books onto their servers is precisely the type of factual issue on which discovery is required because it is a highly complex technical question where the facts are largely within Defendants' sole possession.

data … transmitted … by a … electromagnetic … system" because the chipsets within the iDevice that cause it to function are electromagnetic systems. The iDevice is also a "system that affects interstate or foreign commerce"; by definition any device that connects to the Internet now affects interstate or foreign commerce within the broad definition of that phrase. The Contacts themselves also affect interstate or foreign commerce. By definition, the Contacts are lists of names and addresses for correspondence across the internet, telephone system, or mail. Plaintiffs also allege that the interception of the Contacts takes place simultaneously with the transfer of the data within the iDevice, thus satisfying any court-imposed simultaneity requirement.[15]

The App Defendants attempt to generate a dispute over the need for simultaneous interception. While preserving their disagreement with this court-generated rule in the event it is later overturned, Plaintiffs pled a simultaneous interception. The App Defendants also argue that there is no allegation that a communication was being sent to or received from a third party. They cite no law to support this argument, and no such requirement exists in the statute.

Each and every element of an ECPA claim is thus satisfied. The App Defendants cannot avoid this properly pled claim by mis-describing it, or by characterizing it as "confused" without actually discussing the claims made.

Finally, The App Defendants attempt to bring themselves within an exception to the ECPA's interception requirement, by arguing that they were intended parties to the unlawful interception they caused. Section 2511(2)(d) provides that it is not unlawful for a person to intercept electronic communication "where such person is a party to the communication…" 18 U.S.C. § 2511(2)(d). The App Defendants attempt to analogize their defense to Crowley v.

---

[15] The App Defendants describe as "nearly identical" the allegations rejected by Judge Gonzalez-Rogers in Hernandez, 2012 WL 5194120 before the case was consolidated with the other cases herein. The factual allegations in Hernandez, however, were substantially less developed on this issue than those presented in Opperman and here after consolidation of the case. Indeed, leave to amend was granted in Hernandez on this claim for precisely that purpose. The prior order in Hernandez thus provides no support for the App Defendants' attempt to dismiss the ECPA claim in this case.

CyberSource Corp., 166 F. Supp. 3d 1263 (N.D Cal. 2001), where the court held that Amazon did not "intercept" email that the plaintiff deliberately sent to it. Id. at 1269. This analogy fails for two reasons. First, nothing in Crowley or any other cases suggests that a defendant is a party to a victim-initiated communication where they have wrongfully and without permission caused the communication to automatically be sent to themselves. In fact, cases in this District come to the opposite conclusion. Facebook, Inc., 844 F. Supp. 2d at 1034 ("To hold that Plaintiff originated the e-mails merely because Facebook servers sent them would ignore the fact that Defendants intentionally caused Facebook's servers to do so, and created a software program specifically designed to achieve that effect."). Second, the initial intercepted communication here was between the storage memory and active application on the iDevice; it was not a communication to the App Defendants. The simultaneous communication over the Internet to the App Defendants (which they initiated without permission) was the wrongful interception.

At bottom, Plaintiffs have alleged that the App Defendants used hidden code, without the permission or knowledge of Plaintiffs, to initiate a communication of the contents of the address book within the iDevice, and then surreptitiously divert that information to themselves over the internet. That is just as much an interception as setting an automatic forward on an email system or using screen capturing spyware that secretly captures and sends screen images. See United States v. Szymuszkiewicz, 622 F.3d 701, 704-06 (7th Cir. 2010); Shefts v. Petrakis, 10-cv-1104, 2012 WL 4049484, *8 (C.D. Cal. Sept. 13, 2012).

b) Texas and California Wiretap Statutes, Cal. Penal Code § 630 et seq.

The App Defendants also seek to dismiss Plaintiffs' claims under the California and Texas Wiretap statutes. Their argument is wholly duplicative of their ECPA argument; they allege that Plaintiffs have not alleged a contemporaneous interception. As discussed above, Plaintiffs have in fact done so. Thus, just as the App Defendants' attack on the ECPA claim fails, so do their attacks on the ECPA's Texas and California analogues.

6. Plaintiffs' Common Law Privacy Claims Are Properly Pled

Plaintiffs have properly pled their common law claims for invasion of privacy and against the App Defendants. As the App Defendants recognize, there are no pertinent differences between California and Texas law on these claims.

a) Intrusion upon seclusion

Intrusion upon seclusion requires: (1) a defendant to intentionally intrude on a plaintiff's solitude, seclusion, or private affairs, and (2) that the intrusion is highly offensive. Billings v. Atkinson, 489 S.W.2d 858, 860 (Tex. 1973); Shulman v. Group W Prods, Inc., 18 Cal.4th 200, 231 (1998). Plaintiffs readily meet that standard. Under Billings, for example, the placing of a listening device onto or bugging a phone was "highly offensive" and actionable as an unwarranted invasion of privacy. What App Defendants did here differs only in that their conduct was more technically advanced.

The CAC alleges in detail that Defendants placed malware apps on Plaintiffs' iDevices that allowed Defendants to obtain, without permission, Plaintiffs' private iDevice Contacts information. (CAC ¶¶ 142-44, 148, 160, 238-245, 259, 262-267, 269-271, 282-283, 290-292, 301-307, 314-322, 325, 329-333, 341, 345-346, 349-352, 355-358, 361-364, 371-377, 388-400, 409, 420-421, 424-425, 428-430, 629-633.)

While the App Defendants do not deny that their conduct was intrusive, they argue it was not "highly offensive" because, they say, there is no allegation that they *used* the misappropriated private information for a "highly offensive purpose." (App Def. MTD at 32.) There is no such requirement in either California or Texas law. Defendants cite no Texas authority on the point, and misread the two California cases on which they rely. First, in Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 993 (2011), the defendant retailer asked customers for their zip codes under false pretenses, then used that information to generate a mailing list for marketing materials. There was a misrepresentation about purpose, not an improper invasion, and the information obtained—zip codes—is not private. Id. at 992. In those circumstances, the only way for the conduct to be "highly offensive" was if the information was

used for an offensive purpose. The court concluded there was not, noting in passing that he other cases finding the "highly offensive" element met also include an offensive use. Id. at 993. That passing dicta does not create a new limitation to this established common law tort. Here, the invasion itself was highly offensive, as was the method of unauthorized access of this highly private information. The Court need not find that Defendants *also* used the information for a highly offensive purpose to find the "highly offensive" element to be properly pled.

Second, the Court's conclusion in In re iPhone Litig., 844 F. Supp. 2d at 1063, that dissemination of certain data was not "highly offensive," did not turn on whether the material was used in a highly offensive purpose. The court did not clearly articulate how it arrived at its conclusion. It appears that the court relied on Folgelstrom, which as described above is distinguishable from the present case, and/or based its conclusion on the finding that the dissemination was, at most, negligent. Id. at 1063. The court cites California case that provides that "negligent conduct that leads to theft of highly personal information" does not give rise to an invasion of privacy claim. Id. In stark contrast here, Plaintiffs have alleged a deliberate, targeted invasion of highly personal and private information – their electronic rolodexes.

Electronically poaching private iDevice Contacts without permission is an act of surveillance, just like secretly tapping a phone. Billings, 489 S.W.2d at 860. It may be that the widespread nature of this misconduct is now coming to light, but the breath and frequency of consumer abuse does not make it a legitimate commercial behavior.

b) Public Disclosure of Private Facts

The CAC also properly pleads a claim for invasion of privacy based upon publicly disclosing private facts. (CAC ¶¶ 128-130, 146, 149-150, 428.) The App Defendants argue that the claim is insufficient because Plaintiffs have not alleged a public disclosure. To the contrary, Plaintiffs specifically allege that every App Defendant acquired private Contacts information, and concurrently disclosed it publicly, including by: (1) publicly broadcasting it over WiFi and sending it, in many instances unencrypted, over the internet, making it publicly available to third parties as well as service providers, (2) sending the information to themselves and using it in

their own business, thus making it available to their information technology personnel, (3) sending it to third party servers and thus making it available to the server system owners, and (4) by using it in their own business. (Id.) The CAC also alleges that defendant Chillingo shared the Contacts data with Rovio and Zepto Labs (or visa versa) and reportedly with Google, Inc. (CAC ¶¶ 274, 381, 393, 396, 398, 408-409.) Defendants may argue that the above constitutes only a "small group," or that system owners and service providers did not have access, but that would be a factual argument that is contradicted by the facts alleged in the complaint, and as such beyond the bounds of a motion to dismiss.[16] Thus, Plaintiffs' allegations state a claim for intrusion.

7. Plaintiffs' Conversion Claim Is Properly Pled

Plaintiffs have properly pled the elements of conversion: (1) that plaintiff owns, legally possesses, or is entitled to possess certain property; and (2) that the defendant unlawfully and without authorization assumed and exercised dominion and control over the property in a manner inconsistent with the plaintiff's rights. See, e.g., Hunt v. Baldwin, 68 S.W. 3d 117, 131 (Tex. 2001); Horton v. Jack, 126 Cal. 521, 526 (1899) (a conversion claim will lie where a person's rights are so invaded that it is justified for him to pay for the property). The CAC alleges – and Apple agrees and advised the App Defendants – Plaintiffs own the iDevice Contacts, which each have intrinsic and commercial value. (CAC ¶¶ 151, 162-171, 20, 6455.) Despite having no right to do so, the App Defendants caused them to be uploaded without authorization, and acquired them wrongfully, unlawfully and in a manner that invaded Plaintiffs' privacy. (CAC ¶¶ 142-44, 148, 151, 160, 162-171, 238-245, 259, 262-267, 282-283, 290-292, 301-307, 314-322, 325, 329-

[16] Defendants' brief also contains a statement that Plaintiffs did not allege any "'private facts' that would be highly objectionable to a person of ordinary sensibilities," but offers no argument in support of that statement. (App Def. MTD at 31.) Courts have repeatedly recognized the extremely private nature of the materials contained on iDevices and similar "smart devices." U.S. v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008); United States v. Wurie, 612 F. Supp. 2d 104, 109 (D. Mass. 2009) (observing that it "seems indisputable that a person has a subjective expectation of privacy in the contents of his or her cell phone").

333, 341, 345-346, 349-352, 355-358, 361-364, 371-377, 388-400, 409, 428-430, 629-633, 649.) Moreover, through this uploading and dissemination, the Defendants usurped the commercial and intrinsic value of these Contacts by stealing them and using them to build their own user base to grow their company, and by de-privatizing them among other things. (CAC ¶¶ 150-51, 167-69.) The App Defendants bring two misplaced challenges. First, they erroneously contend that there is no claim for conversion for the type of property at issue here. Second, they argue that merely *copying* data does not give rise to a conversion claim because that does not deprive the plaintiff of exclusive possession and control. Both contentions are simply wrong.

Under Texas law, a conversion claim lies where the defendant improperly copied electronic data. Yazoo Pipeline Co., L.P., v. New Concept Energy, Inc., 459 B.R. 636, 653 (S.D. Tex. 2011). In Yazoo, just like here, the defendants argued that electronic data was intangible property that could not be converted under Texas law. Id. The court rejected that contention, holding that when electronic data is connected in some way to tangible property, which when it is stored in a physical medium (such as on an iDevice) and can be accessed in a manner analogous to the access of traditional property, it can be subject to conversion. Id. at 652; see also Staton Holdings, Inc. v. First Data Corp., 3:04-CV-2321-P, 2005 WL 1164179, *5-*6 (N.D. Tex. May 11, 2005) (holding that an intangible telephone number that was of immense potential value can be converted). Further, Yazoo also squarely rejected the argument, identical to that made here, that merely copying was not conversion. "The Plaintiffs' allegation that [defendant] caused the 'copying' of the data is sufficient. Texas conversion law does not require exclusive control of property. Rather, it recognizes conversion where the defendant exercises dominion and control of the property to the exclusion of *or inconsistent with* the owner's rights." Yazoo, 459 B.R. at 653-4 (internal quotations and citations omitted).

On both points, California law is in accord. Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003), cited by the Defendants, expressly holds that intangible property, there a domain name, can form the basis for a conversion claim. Id. at 1030 (emphasis added) (finding that a domain name meets a three part test for determining the existence of a property right: 1) the interest must be defined; 2) the interest must be subject to exclusive possession and control; and 3) the

putative owner must have established a claim to exclusivity). Like the domain name at issue in Kremen, Contacts data is clearly defined as it is bundled together in the user's Contacts folder and consists of readily identifiable fields. The user invests time in generating, creating, and maintaining on the iDevice the Contacts, which gives them a legitimate claim to exclusivity. Further, the Contacts are certainly capable of exclusive possession and control (after all, Apple purports to provide protections allowing users to maintain that exclusive possession and control). Id. at 1032 (noting that a rolodex could be the subject of conversion). Further, under California law, "[i]t is not necessary that there be a manual taking of the property; it is only necessary to show an assumption of control or ownership over the property, or that the alleged converter has applied the property to his own use." Oakdale Village Group v. Fong, 43 Cal. App. 4th 539, 543 (1996).

"[F]undamental to the concept of ownership of personal property is the right to exclude others." eBay, Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058, 1066-67 (N.D. Cal. 2000) (citing Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (characterizing "the right to exclude others" as "one of the most essential sticks in the bundle of rights that are commonly characterized as property)). A physical address book can be put in a safe and locked away; cracking the safe and taking the book (or copying its Contacts) would clearly be conversion—there is no reason for a different result merely because the same Contacts dataset and data exists in electronic form rather than paper form. Defendants' motion to dismiss the California and Texas conversion claims should be denied.[17]

8. Plaintiffs Properly Pled Their Trespass To Chattels Claim

Under Texas law, the wrongful interference with the use or possession of another's property constitutes actionable trespass. Omnibus Int'l, Inc. v. AT&T, Inc., 111 S.W. 3d 818, 826 (Tex. 2003). Liability arises when there are actual damages to the property or the owner is

[17] Judge Rogers' decision in Hernandez does not mandate a different result. Unlike the situation here, the Hernandez plaintiff did not at that time allege that Path wrongfully interfered, dispossessed him of, or exercised any dominion or control over his address book.

deprived of its use for a period of time. Zapata v. Ford Motor Credit Co., 615 S.W. 2d 198, 201 (Tex. 1981). Under California law, trespass to chattels lies where an intentional interference or intermeddling with the possession of personal property has proximately caused injury. Intel v Hamidi, 30 Cal. 4th 1342, 1350-51 (2003); eBay, Inc., 100 F. Supp. 2d at, 1065, 1071 ("Where the conduct complained of does not amount to a substantial interference with possession or the right thereto, but consists of intermeddling with or use of or damages to the personal property, the owner has a cause of action for trespass or case, and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use …. [E]ven if [d]efendant only used a small amount of Bay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purpose."). As the App Defendants wrongfully interfered with and used Plaintiffs' tangible property (their iDevices) and Plaintiffs' intangible property (their Contacts), Plaintiffs allege viable trespass claims under Texas and California law. (CAC ¶¶ 7, 135, 147-151, 428-433, 652, 662-671.)

The CAC alleges that the App Defendants, without Plaintiffs' consent, placed malware on Plaintiffs' iDevices, which made those iDevices initiate "calls" and enabled the App Defendants to unlawfully spy on Plaintiffs and acquire Plaintiffs' Contacts. (Id.) The App Defendants captured and disseminated Plaintiffs' Contacts to unauthorized recipients and servers via the internet. (Id.) Defendants not only made Plaintiffs' iDevice function counter to Plaintiffs' intent, the App Defendants did this secretly and without consent, and unjustly benefitted and profited at Plaintiffs' detriment and expense. (Id.); see also Baugh v. CBS, Inc., 828 F. Supp. 745, 756 (N.D. Cal. 1993) ("In general, California does recognize a trespass claim where the defendant exceeds the scope of the consent.") (cited in eBay, Inc., 100 F. Supp. 2d at 1070).

Thus, the App Defendants did impair the functioning of Plaintiffs' iDevice and interfered in a tangible, real way with the operations of the iDevice and the Contacts. (CAC ¶¶ 428, 652, 662-671.) Their conduct also depleted the users' iDevice battery life and resources like memory, energy, and the useful life of the device, and transformed the Contacts from a private list controlled by Plaintiff to one whose further distribution the Plaintiff cannot control. The App

Defendants also benefitted by taking the commercial value of the Contacts, and damaged the iDevices by infecting them with spyware requiring removal by a qualified technician—all at significant cost to Plaintiffs. (CAC ¶¶ 659-671.)

Thus, Plaintiffs have alleged that they experienced damage (including loss of value) and have stated facts sufficient at this stage for the Court to infer both additional actual damages as well as substantial interference with Plaintiffs' use and possession of their private Contacts data and iDevices.[18] eBay, Inc., 100 F. Supp. 2d at 1070-71.

9. Texas Theft Liability Act, Tex. Civ. Prop. & Rem Code § 134.001; Tex. Pen. Code § 31.03

The elements of a Texas Theft Liability Act claim are the elements of the alleged violation of the Texas Penal Code under which the claim is brought.[19] Plaintiffs' premise their theft liability claim on section § 31.03 (wrongful appropriation of property). Under § 31.03(a), a person commits an offense if he unlawfully appropriates property with intent to deprive the owner of the property. See Tex. Pen. Code § 31.03(a). Appropriation of property is unlawful when it is without the owner's effective consent. Id., at § 31.03(b). As discussed above in detail, Plaintiffs allege that the App Defendants took and appropriated their Contacts without their effective consent. Specifically, Plaintiffs did not consent to the App Defendants obtaining or via their apps causing the transmission or upload of their private iDevice Contacts. (CAC ¶¶ 673-675.) Accordingly, Plaintiffs have adequately pled a claim under § 31.03 of the Texas Theft Liability Act.

---

[18] Plaintiffs consent to install apps was not consent to the installation of a Trojan horse on their iDevice that would secretly take their iDevice address book information, flagrantly violate their privacy and harm their property. (CAC ¶¶ 7, 135, 146-151, 428-433, 652, 662-67.) In fact, the App Defendants promised them the exact opposite—that the apps and products that would not steal their private information. (CAC ¶ 135.)

[19] The Act defines "theft" as unlawfully appropriating or unlawfully obtaining property or services as described by Section 31.03, 33.04, 33.05, 33.06, 33.07, 33.08, 33.09, 33.10, 33.11, 33.12, 33.13, and 33.14 of the Texas Penal Code.

The App Defendants' arguments against this claim are the same as they make to the previously discussed claims: an insistence that Plaintiffs were not deprived of any property. These arguments are no more successful here than on the prior claims, and the App Defendants' motion to dismiss this claim should be denied.

10. Misappropriation

Under California law, misappropriation falls under the umbrella of unfair competition and requires only that: (1) Plaintiffs spent time, skill or resources in creating the private Contacts data; (2) Defendants acquired, appropriated or used the private data at little or no cost to Defendants; (3) Defendants lacked Plaintiffs' consent; and (4) Defendants' conduct injured Plaintiffs. U.S. Golf Ass'n v. Arroyo Software, 99 Cal. 5th 607, 618 (1999).[20]

Plaintiffs CAC sets out facts underlying each of these elements. Plaintiffs spent significant time compiling their Contacts, the App Defendants acquired, appropriated and used the Contacts at little or no cost to them, the use was without Plaintiffs' consent, and Plaintiffs were injured as their privacy rights were violated, their private iDevice address books deprivatized, and the App Defendants took property worth between $60 and $17,000 –depending on which estimate a jury determines is more accurate – had the App Defendants paid fair market value. (CAC ¶¶ 151, 165-168, 680-684). Rather than accepting Plaintiffs' allegations as true, the App Defendants ignore Plaintiffs' pleadings and mistakenly contend that Plaintiffs did not take the requisite time or make the requisite effort to create their Contacts. Per the CAC, Plaintiffs' private Contacts data took substantial time to amass and create over Plaintiffs' lives. (CAC ¶¶ 151, 160, 162-171.)

[20] Under Texas law, the elements of misappropriation are similar, namely that (1) Plaintiffs created information or products through extensive time, labor, skill and/or money; (2) Defendants used the information or product in competition with plaintiff, such that defendant gained a "free ride" because it was burdened with little or none of the expense or time incurred by plaintiff to create it; and (3) Plaintiffs suffered commercial damage. U.S. Sporting Products, Inc. v. Johnny Stewart Game Calls, Inc., 865 S.W. 2d 214, 217 (Tex. 1993).

Next, the App Defendants contend that Plaintiffs have not alleged that they suffered commercial damage. But Plaintiffs did allege this. (CAC ¶¶ 151, 160, 162-171, 680-684.) Moreover, the App Defendants, like Plaintiffs, are now using the information in Plaintiffs' Contacts to communicate with Plaintiffs' social network of contacts; thus, they each are using these materials commercially "in competition" with one another. (Id.) The reasonable inference is that the App Defendants did, as pled by Plaintiffs, gain a free ride as they effectively used the contents of the ill-gotten Contacts. Plaintiffs had property that they valued, that the App Defendants valued, and that also had significant market value. (Id.) The App Defendants had a choice to steal it or seek to purchase it for a fair market value. They chose to take and then use Plaintiffs' Contacts and, therefore, obtained a "free ride." Thus, Plaintiffs state a viable misappropriation claim under Texas and California law.

11. Negligence

Plaintiffs' negligence claim is also well pleaded. The App Defendants owe a duty under societal norms, statutes, industry standards and the criminal law, to exercise reasonable care and operate according to industry accepted standards. (CAC ¶¶ 198-207.) The App Defendants should not have acquired or caused the transmission or upload of Plaintiffs' Contacts without prior permission. Nor should they have made and sold malware products or kept knowledge about their apps' malicious functions from Plaintiffs and the public. By selling and providing flawed products and infecting Plaintiffs' iDevices with malware, which invaded their privacy, converted their property and disseminated their private Contacts without permission, the App Defendants breached their duty and Plaintiffs suffered damages. (CAC ¶¶ 142-44, 148, 151, 160, 162-171, 238-245, 259, 262-267, 282-283, 290-292, 301-307, 314-322, 325, 329-333, 341, 345-346, 349-352, 355-358, 361-364, 371-377, 388-400, 409, 428-430, 629-633.) As a consequence, Plaintiffs' claim for negligence should proceed.

Significantly, one of the Defendants here, Path, Inc. previously raised the identical argument under California law in the case Apple seeks to transfer into, only to have it rejected. As noted by Judge Rogers when she denied Path's motion to dismiss, the In re iPhone Litig.

ruling does not exempt app developers from their own negligence when their failure to exercise reasonable care causes injuries. See Hernandez, 2012 WL 5194120 at *6.

Texas law, too, is quite clear. Every person has a duty to exercise reasonable care to avoid injury to others. Midwest Emp'rs Cas. Co. ex. English v. Harpole, 293 S.W. 3d 770, 776 (Tex. 2009). Foreseeability of risk is a primary factor in determining whether a duty exists. Greater Houston Tran. Co. v. Phillips, 801 S.W.2d 523, 525 (Tex. 1990). Here, the risk of harm was certain. That Defendants seriously argue they may take property that does not belong to them, and have no duty otherwise, defies reason.

As discussed above, the App Defendants have also violated numerous statutes, including criminal laws, such that their actions constitute negligence *per se*. As it is well settled that negligence per se can be premised on the violation of a criminal statute, and as plaintiffs are the type of people these statutes were designed to protect, and as the non-consensual uploading of Plaintiffs' address books injured Plaintiffs and their property, Plaintiffs raised a valid negligence *per se* claim. See, e.g., Perry v. S.N., 973 S.W.2d 301, 304-06 (Tex. 1998) ("The threshold questions in every negligence per se case are whether the plaintiff belongs to the class that the statute was intended to protect and whether the plaintiff's injury is of a type that the statute was designed to prevent").[21]

Nevertheless, the App Defendants again ignore Plaintiffs' pleadings altogether and claim (1) that Plaintiffs have not alleged that they suffered any damages; and (2) that even if they did, the negligence claims would barred by the economic loss rule. They are wrong on both counts. This brief has already repeatedly explained how Plaintiffs were damaged by the App Defendants' conduct. As for the economic loss doctrine, it does not preclude Plaintiffs' negligence claims against the App Defendants. In fact, it is well settled that the economic loss rule does not apply if Plaintiffs allege – as they do here – that Defendants violated their duty not to commit intentional torts or crimes or that the App Defendants knew their actions would cause

[21] Gross negligence merely requires a party's actions involve an extreme degree of risk of harm and conscious disregard of that risk. Lee Lewis Const., Inc. v. Harrison, 70 S.W.3d 778, 785 (Tex. 2001). Plaintiffs' allegations state these elements. See CAC generally.

unmitigatable harm. Wine Bottle Recycling LLC v. Niagra Sustems, 12-1924 SC, 2013 WL 5402072, *4 (N.D. Cal. Sept. 26, 2013) (citing Robinson Helicopter Co., Inc. v. Dana Corp., 34 Cal.4th 988, 990 (2004)). This is not a case in which Plaintiffs are trying to transform a contractual claim into a tort action. Rather, Plaintiffs' negligence claims stand on their own. The App Defendants' motion to dismiss them should be denied.

IV. CONCLUSION

For the foregoing reasons, the Court should deny Defendants' 12(b)(6) motions to dismiss except with respect to the RICO and vicarious liability claims.[22] Alternatively, to the extent the Court finds aspects of Plaintiffs' other claims deficient, Plaintiffs would respectfully ask the Court to grant it leave to remedy any such deficiencies in an amended pleading.

DATED: December 2, 2013 **KERR & WAGSTAFFE LLP**

By: s/ Michael Ng
MICHAEL NG

Attorneys for *Opperman* Plaintiffs

Dated: December 2, 2013

By */s/ David M. Given*
David M. Given
Nicholas A. Carlin
PHILLIPS, ERLEWINE & GIVEN LLP
50 California Street, 32nd Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911

By */s/ James M. Wagstaffe*
James M. Wagstaffe
Michael K. Ng
Ivo M. Labar
Michael J. Von Loewenfeldt
KERR & WAGSTAFFE LLP

[22] Plaintiffs believe the RICO and vicarious liability claims are well pleaded. However, in light of Defendants' clear liability on the numerous other claims based on the same facts, Plaintiffs elect not to prosecute these claims at this time and have no objection to their dismissal without prejudice as to these Defendants.

100 Spear Street, 18th Floor
San Francisco, CA 94105
Tel: 415-371-8500
Fax: 415-371-0500

Interim Co-Lead Counsel for Plaintiffs

Carl F. Schwenker (TBN 00788374,)
LAW OFFICES OF CARL F. SCHWENKER
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Tel: 512.480.8427
Fax: 512.857.1294
Email: cfslaw@swbell.net

Plaintiffs' Liaison Counsel

Jeff Edwards (TBN 24014406; *pro hac vice*)
EDWARDS LAW
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Telephone: 512.623.7727
Facsimile: 512.623.7729

Jennifer Sarnelli
James S. Notis
Gardy & Notis LLP
560 Sylvan Avenue
Englewood Cliffs, NJ 07632
Email: jsarnelli@gardylaw.com
jnotis@gardylaw.com

Plaintiffs' Steering Committee ("PSC")